ReQuest2

Hi all,

Last week I sent an email about a burp extension to intercept and decode SAML requests. Well, now it also supports intruder attacks.

In brief: the extension SAMLReQuest decodes SAML authentication requests and displays them in a sub-tab in Proxy- History, Proxy-Intercept and also Repeater. In case of Proxy-Intercept and Repeater, if you change the decoded SAML authentication request, the changes get reflected automatically in the original request.

Now the extension provides automatic attacks using Intruder!

In any SAMLReQuest sub-tab, there is a button at the bottom of the sub-tab called “Send Decoded Request to Intruder“ as shown in Figure 1. The chosen request was successful and its response was 302 Redirect.

*Figure 1: "Send Decoded Request to Intruder" button*

The request in Intruder is the same as the original one, except that SAMLRequest parameter is decoded as shown in Figure 2. You can set the payload positions and payloads as in any normal request. In Figure 2, I will change the last four characters in ID parameter of SAML authentication request.

*Figure 2: Decoded SAML request in Intruder*

In the results of intruder, the SAMLRequest parameter is also decoded. But of course the parameter would be seen properly encoded in Wireshark.

Figure 3 shows the results of the above intruder test on Shobboleth VMs. The original request was rejected when resent again (200 OK but with error) and the other 2 requests were accepted (302 Redirection, as the response to the original successful request).

*Figure 3: Intruder results*

Note: When a request is sent to intruder, it is configured to send the request over HTTPS. So in case the system under test uses HTTP and not HTTPS, don't forget to change that in Intruder-Target tab.

asdsa